УТВЕРЖДЕНО

Решением Правления ООО НКО «ПэйПал РУ»

13 ноября 2015 г. (Протокол №6/2015-П)

Приказ Председателя Правления

ООО НКО «ПэйПал РУ»

от 13.11.2015 № 21-ОД

APPROVED BY

Resolution of the Management Board of LLC NBCI "PayPal RU"

dated November 13, 2015 (Minutes No.6/2015-P)

Order of the Chairperson of the Management Board

of LLC NBCI "PayPal RU"

dated 13.11.2015 No. 21-OD

ПАМЯТКА КЛИЕНТУ (РЕКОМЕНДАЦИИ ООО НКО «ПЭЙПАЛ РУ» ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА) ООО НКО «ПЭЙПАЛ РУ»

HANDOUT FOR CLIENTS (GUIDELINES OF LLC NBCI "PAYPAL RU" FOR PROTECTING THE INFORMATION FROM UNAUTHORIZED ACCESS)

LLC NBCI "PayPal RU"

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

LIST OF TERMS AND ABBREVIATIONS

Антивирусная защита	Комплекс программно-технических средств, который позволяет определить наличие вредоносного кода среди обрабатываемых электронными вычислительными машинами приложений и файлов, идентифицировать его и исключить соответствующим методом	**Antivirus security**	A set of software and hardware facilities which detect malicious code among the applications and files processed by computing tools, identify and eliminate such malicious code
Информация	Сведения (сообщения, данные) независимо от формы их представления	**Information**	Information (messages, data) regardless of its presentation form
Компьютерный вирус	Программа, вызывающая нарушение работы других программ, порчу информации, невозможность прочитать файлы, замедление либо нестабильность работы электронных вычислительных машин	**Computer virus**	A software facility that causes the malfunctions of other software facilities, damage of information, failure to read the files, slowdown or instability of operation of computing tools.
Программное обеспечение (ПО)	Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ	**Software**	A collection of software facilities of the information processing system and the program documents required for operation of these software facilities
НКО	Общество с ограниченной ответственностью Небанковская кредитная	**NBCI**	Limited Liability Company Non-Banking Credit Institution "PayPal RU"

	организация «ПэйПал РУ»		
Группа PayPal	Совокупность физических и юридических лиц, входящих в одну группу с PayPal Holdings Inc (ПэйПал Холдингс Инк).	**PayPal group**	Individuals and legal entities being members of the same group as PayPal Holdings Inc.
Учетные данные	Имя пользователя и пароль.	**Credentials**	Username and password.

СОДЕРЖАНИЕ

CONTENTS

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ содержит рекомендации к организации защиты информации клиентов от неправомерного и несанкционированного доступа к данной информации.

1.2. Настоящий документ должен быть доступен для ознакомления Клиентами НКО.

1.3. Под кражей учетных данных понимается хищение личных данных клиента НКО и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.4. При осуществлении защиты информации основными задачами являются предотвращение злонамеренных воздействий, а в случае их наступления - минимизация причиненного ущерба. Для обеспечения надлежащей степени защищенности необходимо использование комплексного подхода, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне НКО, так и на стороне клиента.

1.5. Риски получения несанкционированного доступа к информации, прежде всего, связаны с фишингом (использованием ложных ресурсов сети Интернет с целью осуществления переводов электронных денежных средств лицами, не обладающими правом распоряжения этими элеткронными денежными средствами), а также воздействием вредоносного кода.

1.6. Под фишингом понимается попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от

1. GENERAL PROVISIONS

1.1. This document contains the recommendations as to organization of protection of the clients' information against unlawful and unauthorized access.

1.2. This document shall be available to the clients of the NBCI.

1.3. Theft of account details means theft of personal data of an NBCI's client and their wrongful use to perform the unauthorized operations on the client's behalf. The optimum way of protection from theft of account details is to learn to recognize the methods of such attacks in order to prevent such situations.

1.4. The information protection primarily aims at preempting the malicious actions and minimizing the damage if they occur. To ensure the proper level of protection, it is required to utilize a comprehensive approach which implies that both the NBCI and the client take sufficient care of the information security issues.

1.5. The risks of unauthorized access to the information primarily refer to phishing (when persons use false Internet resources to make transfers of the electronic money they have no right to dispose of) and malicious code.

1.6. Phishing means attempt to intercept a client's personal data. One of the most common ways of phishing is when the fraudsters send the e-mails on behalf of a known company. These e-mails typically contain a link to the insecure website page. On this page you will be offered to enter your personal data. You may think that it is secure,

мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

while in fact the fraudsters are stealing your information.

1.7. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификации ПО либо на перехват информации, в том числе паролей.

1.7. The antivirus security is established to eliminate the possibility of infection of personal computers used to access the system with viruses and malware, which are meant to destroy, cause malfunction or modify the software, or intercept the information, including passwords.

1.8. Средства и методы защиты информации, применяемые в НКО, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов электронных денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

1.8. The facilities and methods for information protection, which are applied at the NBCI, allow to ensure the required security level during electronic money transfers and prevent the fraudulent withdrawal of funds from the clients' accounts. This security level can be ensured only if the clients comply with the requirements stated in this document.

2. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО КОДА

2. RECOMMENDATIONS ON INFORMATION PROTECTION FROM THE MALICIOUS CODE

2.1. На Вашем персональном компьютере (Компьютере клиента) должно быть установлено антивирусное ПО, при наличии технической возможности его установления.

2.1. If technical capacity allows, your personal computer (the client's computer) shall be equipped with the antivirus software.

2.2. Антивирусное ПО необходимо регулярно обновлять. Рекомендуется также установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении компьютерных вирусов. Лечение (удаление) зараженных файлов должно производиться антивирусным средством в автоматическом режиме.

2.2. The antivirus software shall be updated regularly. It is also recommended to set by default the maximum level of security policies, i.e. the one that does not require user attention when a computer virus is detected. The antivirus facility shall cure (delete) the infected files automatically.

2.3. Не реже одного раза в неделю в автоматическом режиме рекомендуется осуществлять полную проверку жесткого диска персонального компьютера на предмет наличия

2.3. At least once a week, it is recommended to perform a complete automated scan of the PC's hard drive for computer viruses. The scanning is

компьютерных вирусов. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

performed as scheduled in the antivirus facility.

2.4. Рекомендуется подвергать антивирусной проверке любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

2.4. It is recommended to scan for viruses any information received or transferred via telecommunication channels, as well as the information on removable media (magnetic media, CDs, DVDs, USB flash drives, etc.). If technical capacity allows, the scanning shall be performed automatically.

2.5. При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов.

2.5. If the Internet is used to exchange e-mails, it is required to apply the antivirus software developed specifically for the mail clients.

2.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) рекомендуется приостановить работу с системой до полного устранения неисправностей.

2.6. In case you suspect the computer virus infection (irregular software operation, appearance of image and sound effects, data distortion, disappearing files, frequent system error alerts, boost of incoming/outgoing traffic, etc.), it is recommended to stop operating the system before complete elimination of faults.

2.7. Старайтесь не использовать компьютер, с которого Вы осуществляете переводы электронных денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (эротические сайты, игровые сайты, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

2.7. Try not to use the computer on which you make electronic money transfers to visit social networks, entertainment and suspicious websites (erotic, gaming, dating, software, music, movie websites, etc.), because these Internet resources are most commonly used to distribute the computer viruses.

2.8. Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

2.8. Do not open the files received via e-mail from unknown senders.

3. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПУТЕМ ИСПОЛЬЗОВАНИЯ ЛОЖНЫХ (ФАЛЬСИФИЦИРОВАННЫХ) РЕСУРСОВ СЕТИ ИНТЕРНЕТ

3.1. Мошенническим (поддельным) web-сайтом является небезопасный web-сайт, на котором Вам предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Вашего банка или НКО), и предназначены для сбора конфиденциальной информации обманным путем.

3.2. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании, отличающийся на один или несколько символов, обычно трудно различимых (например, буква «о» заменяется цифрой «0»).

3.3. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это электронное письмо, отправленное мошенниками.

3.4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме НКО всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.5. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и

3. RECOMMENDATIONS ON PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS VIA FALSE INTERNET RESOURCES

3.1. A fraudulent (fake) website is an unsecured website asking you to enter the confidential information. These websites are often almost identical to the websites of known companies that you trust (e.g. your bank or the NBCI) and serve for fraudulent acquisition of confidential information.

3.2. Always check the sender address before viewing the e-mail. The line "From" may contain an e-mail address in the official format that is nearly identical to the address of a real company but differs in one or several characters, which are usually hard to detect (e.g. letter "o" is replaced with "0").

3.3. Read the e-mail contents carefully. The e-mails form known companies never have orthographic or grammar mistakes. If you see foreign words, special symbols, etc., this e-mail may be sent by fraudsters.

3.4. Beware of impersonal address, such as "Dear User",. or address by e-mail address. In a real e-mail, the NBCI always refers to you by name and surname or a company name. The typical phishing e-mail starts with impersonal address.

3.5. Try to keep calm. Many fraudulent e-mails contain calls for immediate action trying to make you act quickly and unreasonably. Many fake e-mails try to convince you that your account will be

необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету угрожает опасность, если Вы немедленно не обновите критически важные данные.

in danger if you don't change the essential data immediately.

3.6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке. НКО всегда направляет Вас к web-страницам, адрес которых начинается с https://. Никогда не переходите по ссылке, начинающейся с http://.

3.6. Analyze the links carefully. The links may be almost identical to the real ones, but they will lead you to a fraudulent website. If a link looks suspicious or does not comply with security requirements (e.g. starts with http:// instead of https://), do not use it. The NBCI always gives you "https://" links. Never use "http://" links.

4. РЕКОМЕНДАЦИИ ПО ПРЕДОТВРАЩЕНИЮ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ТРЕТЬИМИ ЛИЦАМИ

4. RECOMMENDATIONS ON PREVENTION OF UNAUTHORIZED ACCESS BY THIRD PARTIES

4.1. Рекомендуем регулярно менять пароль для работы со своим счетом PayPal. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.1. It is recommended to regularly change the password of your PayPal account. Your password shall contain at least eight characters and form a complex combination of upper- and lower-case letters, digits, and symbols.

4.2. Рекомендуется использовать различные уникальные пароли для различных web-сайтов, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем счете PayPal, банковском счете и т. д.).

4.2. It is recommended to use different unique passwords for different websites where you enter the confidential data (e.g. the details of your PayPal account, bank account, etc.).

4.3. В том случае, если Вы обнаружили, что Ваш пароль от счета PayPal скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 4.1.

4.3. In case you discover that your access password for PayPal account has been compromised, immediately change it to a new one that is known to you only and complies with the requirements listed in Item 4.1.

4.4. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в счет PayPal, необходимо как можно быстрее восстановить доступ к счету PayPal через систему восстановления пароля.

4.4. In case you discover that the password used for previous access is no longer valid and does not allow you to login to PayPal account, it is required to restore the access to PayPal account through the password recovery system as soon as possible.

4.5. Не разглашайте свой пароль от системы

4.5. Do not disclose your password to anyone,

никому, даже близким друзьям или членам семьи. НКО не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные.

4.6. Не пересылайте файлы с конфиденциальной информацией для работы с счетом PayPal по электронной почте или через SMS-сообщения.

4.7. Рекомендуем исключить возможность доступа к компьютеру, с которого Вы осуществляете работу в системе, посторонних лиц.

4.8. Незамедлительно обращайтесь в службу поддержки (тел. 8-800-333-2676) в том случае, если Вы получили уведомление системы об операции, которую Вы не проводили.

even your family or close friends. The NBCI does not send the e-mails, text messages or other messages with a request to update your confidential data.

4.6. Do not send the files with confidential information for access to PayPal account via e-mails or text messages.

4.7. It is recommended that you restrict third-party access to the computer on which you work with the system.

4.8. If you receive a system notification about an operation you did not make, immediately contact the support (tel. 8-800-333-2676).